REMARKS/ARGUMENTS

Claims 1-26 and 28-32 are pending and remain rejected under 35 U.S.C. §103(a) as being unpatentable over Grube et al. in view of Anderson, Jr.

By the present Amendment, Applicants have amended claims 1, 13, 20, 21, 31, and 32, in order to clarify such claims by highlighting the existing limitations that made such claims distinguishable over the cited references. As to the changes to independent claims 1, 20, 21, 31 and 32, Applicants respectfully request that such amendments be entered, inasmuch as the added clarifying language was clearly implicit in the claims (prior to amendment), does not change the scope of the claims, and thus would not require additional searching by the Examiner. Dependent claim 13 now includes the limitation of a "set-top box" retrieving the first and second indicators. Support for such language can be found in the specification, e.g., page 7, lines 25-28).

In independent claim 1, Applicants now recite a method including the steps (among others) of:

"receiving a first indicator... that instructs the system to operate at a higher level of security;"

"retrieving a separate, second indicator... for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator;" and

"preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator; while

continuing operation of said processing system."

Grube, the primary reference relied on by the Examiner, discloses a system for preventing unauthorized monitoring of wireless data transmissions, where communication units 114, 115 request data from databases 105, 106 through a security gateway 103. The security gateway 103 determines the level of security required for transmissions based on the type of data requested, the identity of the requesting unit, and the identity of the targeted database (col. 3, lines 45-49). The security gateway 103 then sends a message informing the communication unit of the required transmission security level, and waits for an acknowledgement from the

communications unit with the required security level parameters. If the acknowledgement is not received, the transmission process ends (col. 7, lines 40-58).

Grube is missing several key elements of Applicants' invention. For example, **Grube** does not disclose a system using two indicators as in Applicants' method and system, including "a first indicator... that instructs the system to operate at a higher level of security" and "a separate, second indicator... for instructing the system to operate at a lower level of security", as recited in claim 1. Further , **Grube** does not disclose "preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator; while continuing operation of said processing system", as also recited in claim 1.

In order to overcome the missing elements of **Grube**, the Examiner combines **Grube** with **Anderson**. **Anderson** discloses a security arrangement 10 for controlling access to a cellular telephone system 11. In order to prevent unauthorized users from attempting to gain access to the system 11, every tenth call has its security level increased by three levels for the duration of that call (col. 12, lines 36-44). In addition, if call information and subscriber call history indicate a potential for fraudulent use (e.g., concurrent calls from same cellular telephone, the called number being a blocked number, etc.), the security level required to make the call can be increased (col. 6, line 40 through col. 7, line 5).

Anderson likewise does not disclose a system using two indicators as in Applicants' method and system, including "a first indicator... that instructs the system to operate at a higher level of security" and "a separate, second indicator... for instructing the system to operate at a lower level of security", as recited in claim 1. Furthermore, **Anderson** does not teach continuing the operation of the system while "preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator", since **Anderson** does not have a second indicator (that instructs the system to operate at a lower level of security).

The Examiner appears to argue that **Grube** does teach two indicators by stating that the first indicator is the information that instructs the system to operate at the higher level (the Examiner appears to find this teaching in **Grube's** disclosure of determining the security level by looking at data type, and the ID of the requesting unit and the destination unit). See

paragraph 3 of the Examiner's remarks. Furthermore, the Examiner appears to argue that **Grube** teaches a second indicator by referencing the failure to receive a proper acknowledgement that results in the process ending in **Grube** (see also paragraph 3 of the Examiner's remarks).

Applicants point out that even if one were to interpret the determination of security level by looking at transmission information as a first indicator (which Applicants disagree with), there is simply no second indicator at all in **Grube**. The acknowledgement message in **Grube** that the Examiner appears to reference in finding the second indicator is clearly not an indicator "for instructing the system to operate at a lower level of security," as in Applicants method of claim 1 (rather the acknowledgment message only permits the transmission to proceed with a higher level of security, and certainly has no feature for lowering the security level).

In addition, in the latest Office Action, the Examiner appears to argue that the second indicator can also be found in **Anderson** (see last few lines of paragraph 4 of the Examiner's remarks, referencing cols. 6 and 7 of **Anderson**, and paragraph 37 of the Examiner's remarks, referencing col. 6 of **Anderson**).

Applicants respectfully disagree. **Anderson** discloses two events that might cause the security level to increase (one event being an increase if there is potentially fraudulent activity as described in cols. 6 and 7). However, no where in **Anderson** is there described a second indicator "for instructing the system to operate at a lower level of security." While it might be argued as implicit in **Anderson** that security levels decrease (after the completion of a call or as preprogrammed and selected by a carrier -- see col. 7, lines 3-5, col. 10, lines 6-17, and col. 12, lines 36-39), there is no separate, second indicator (received from information from an outside source) that instructs the system to operate at a lower level of security, nor is there a step for "preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator," as also recited in claim 1.

Independent claims 20, 21, 31 and 32 are believed allowable for the same reasons as stated above. For example, claim 20 recites a system "operating the system at the high level of security in response to a first security message" and " continuing operation of the system at

the high level of security until an encrypted, second authorization message is received by the system." Similar limitations are found in claims 21, 31 and 32.

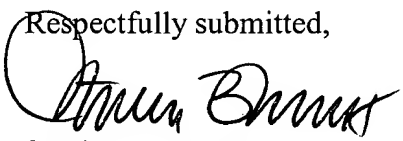
Likewise, the dependent claims (2-19 and 22-30) are allowable for the same reasons as stated above.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



Stephen F. Jewett
Reg. No. 27,565

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
SFJ/bhr
60566660 v1